(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－91883
（P2002－91883A）
(43)公開日　平成14年３月29日(2002.3.29)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	13/00	６２５	Ｇ０６Ｆ 13/00	６２５	５Ｋ０２７
Ｈ０４Ｌ	12/54		Ｈ０４Ｍ 1/00	Ｒ	５Ｋ０３０
	12/58		11/00	３０２	５Ｋ１０１
Ｈ０４Ｍ	1/00		Ｈ０４Ｌ 11/20	１０１Ｂ	
	11/00	３０２			

審査請求　未請求　請求項の数11　ＯＬ　（全 24 頁）

(21)出願番号　特願2000－284861(P2000－284861)

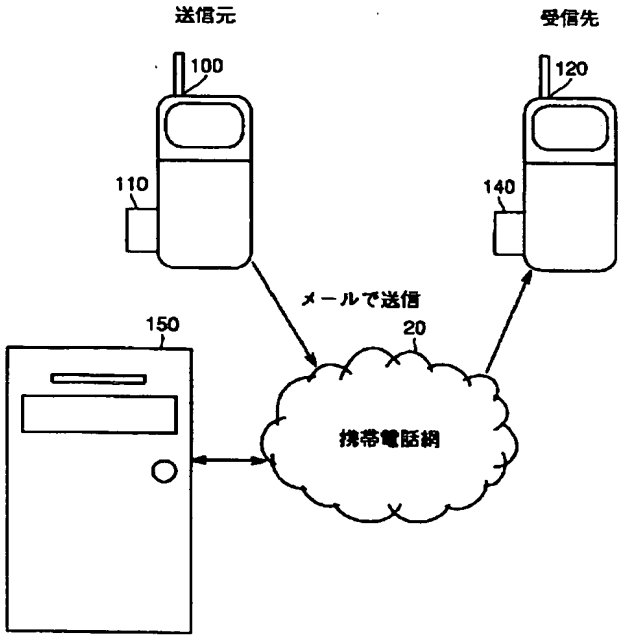
(22)出願日　平成12年９月20日(2000.9.20)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　太田　晴也
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

Ｆターム(参考)　5K027 AA11 BB09 HH00 MM03
5K030 GA19 HA06 HC09 JL01 JT01
JT02 JT09 KA01 KA02 LD13
5K101 KK02 KK18 LL12 NN15

(54)【発明の名称】　データ配信システムおよびデータ端末装置

(57)【要約】
【課題】　ユーザ間でコンテンツ情報を自由にやり取りすることができるデータ配信システムおよびそのデータ配信システムに用いられるデータ端末装置を提供する。
【解決手段】　携帯電話機１００は、コンテンツデータと、コンテンツデータの関連情報であるコンテンツ情報とを含むコンテンツファイルをサーバからダウンロードし、装着されたメモリカード１１０に記録する。そして、携帯電話機１００は、メモリカード１１０からコンテンツ情報を読出し、その読出したコンテンツ情報をメール文に付加したコンテンツメールを作成し、携帯電話網２０およびメールサーバ１５０を介して携帯電話機１２０へ送信する。



【特許請求の範囲】

【請求項１】　コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとを保持するサーバと、
前記サーバから前記コンテンツファイルおよび前記ライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、前記コンテンツファイルに含まれるコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、
前記コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成るデータ配信システム。

【請求項２】　コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとを保持するサーバと、
前記サーバから前記コンテンツファイルおよび前記ライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、前記コンテンツファイルに含まれるコンテンツ情報とコンテンツＩＤとをタグとともにメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、
前記コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成るデータ配信システム。

【請求項３】　コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとを保持するサーバと、
前記サーバから前記コンテンツファイルおよび前記ライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、前記コンテンツファイルに含まれるコンテンツ情報とコンテンツＩＤとをタグとともにメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、
前記コンテンツメールを受信し、その受信したコンテンツメールに含まれるコンテンツＩＤを前記サーバへ送信して前記サーバから前記コンテンツＩＤによって特定されるコンテンツファイルをダウンロードする他の端末装置と、
前記メールサーバから前記コンテンツメールを受信し、その受信したコンテンツメールを前記他の端末装置へ送信するメールサーバとから成るデータ配信システム。

【請求項４】　前記データ端末装置は、前記他の端末装置からのコンテンツ情報の送信要求に応じて前記コンテンツメールを出力する、請求項１から請求項３のいずれか１項に記載のデータ配信システム。

【請求項５】　前記データ端末装置は、ユーザによって入力されたコンテンツ情報の送信要求に応じて前記コンテンツメールを出力する、請求項１から請求項３のいずれか１項に記載のデータ配信システム。

【請求項６】　コンテンツデータをファイル形式によって保持するコンテンツファイルと、前記コンテンツファイルを利用するためのライセンスとをサーバからダウンロードしてデータ記録装置に記録し、前記コンテンツファイルに含まれるコンテンツ情報を他の端末装置へ送信するデータ端末装置であって、
バスと、
前記バスに接続され、前記データ記録装置と前記バスとの間でデータのやり取りを制御するインタフェースと、
前記バスに接続され、外部と通信を行なう送受信部と、
前記バスに接続され、情報を入力するためのキー操作部と、
前記バスに接続され、前記他の端末装置へ送信するためのメールを作成するメール作成部と、
前記バスに接続された制御部とを備え、
前記コンテンツファイルのダウンロード時、
前記制御部は、前記キー操作部から入力された前記コンテンツファイルのダウンロード要求に応じて、前記コンテンツデータを特定するためのコンテンツＩＤを前記サーバへ送信するように前記送受信部を制御し、前記送受信部が受信したコンテンツファイルおよびライセンスを前記インタフェースを介して前記データ記録装置へ出力し、
前記送受信部は、前記制御部からの制御により前記コンテンツＩＤを前記サーバへ送信し、前記コンテンツファイルおよび前記ライセンスを受信し、
前記コンテンツ情報の送信時、
前記制御部は、コンテンツ情報の送信要求に応じて、前記インタフェースを介して前記データ記録装置からコンテンツ情報を取得し、その取得したコンテンツ情報を前記メール作成部へ与え、前記メール作成部から出力された前記コンテンツ情報を含むコンテンツメールを前記他の端末装置へ送信するように前記送受信部を制御し、
前記メール作成部は、前記コンテンツ情報をメール文に付加したコンテンツメールを作成し、
前記送受信部は、前記制御部からの制御によって前記コンテンツメールを前記他の装置へ送信する、データ端末装置。

【請求項７】　前記コンテンツ情報の送信時、
前記制御部は、前記キー操作部から入力されたコンテンツ情報の送信要求に応じて、前記コンテンツ情報を前記データ記録装置から取得する、請求項６に記載のデータ

端末装置。

【請求項８】　前記コンテンツ情報の送信時、
前記制御部は、前記送受信部が受信したコンテンツ情報の送信要求に応じて、前記コンテンツ情報を前記データ記録装置から取得する、請求項６に記載のデータ端末装置。

【請求項９】　前記コンテンツ情報の送信時、
前記制御部は、前記インタフェースを介して複数のデータ記録装置からコンテンツ情報を取得し、前記メール作成部へ与える、請求項６から請求項８のいずれか１項に記載のデータ端末装置。

【請求項１０】　前記コンテンツ情報の送信時、
前記制御部は、前記インタフェースを介してユーザが保持する全てのデータ記録装置からコンテンツ情報を取得し、前記メール作成部へ与える、請求項６から請求項８のいずれか１項に記載のデータ端末装置。

【請求項１１】　前記コンテンツ情報の送信時、
前記制御部は、前記コンテンツ情報とともにコンテンツＩＤを前記インタフェースを介して前記データ記録装置から取得し、前記コンテンツ情報およびコンテンツＩＤを前記メール作成部へ与え、
前記メール作成部は、前記コンテンツ情報およびコンテンツＩＤをタグとともにメール文に付加してコンテンツメールを作成する、請求項６から請求項１０のいずれか１項に記載のデータ端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システム、およびそのデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスキーを送信する。そして、暗号化コンテンツデータやライセンスキーを配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンスキーと暗号化コンテンツデ

ータをメモリに記録する。

【００１２】そして、メモリに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。そして、携帯電話機のユーザは、受信した暗号化コンテンツデータを再生した結果、その暗号化コンテンツデータを他人にプレゼントしたい場合がある。また、他人が持っている暗号化コンテンツデータを貰いたい場合もある。さらに、暗号化コンテンツデータに限らず、暗号化されていない平文のコンテンツデータについても、他人との間でやり取りを行ないたい場合がある。

【００１４】

【発明が解決しようとする課題】しかし、コンテンツデータを配信する従来のシステムにおいては、サーバからダウンロードしたコンテンツデータのタイトル、およびアーティスト名等、コンテンツデータの関連情報であるコンテンツ情報を他人に送信したり、他人から受信したりすることがなく、ユーザ間でコンテンツ情報をやり取りすることができないという問題があった。

【００１５】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、ユーザ間でコンテンツ情報を自由にやり取りすることができるデータ配信システムおよびそのデータ配信システムに用いられるデータ端末装置を提供することである。

【００１６】

【課題を解決するための手段および発明の効果】この発明によるデータ配信システムは、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとを保持するサーバと、サーバからコンテンツファイルおよびライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、コンテンツファイルに含まれるコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成る。

【００１７】この発明によるデータ配信システムにおいては、データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および／または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報を取得し、そのコンテンツ情報をメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【００１８】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できる。

【００１９】また、この発明によるデータ配信システムは、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとを保持するサーバと、サーバからコンテンツファイルおよびライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、コンテンツファイルに含まれるコンテンツ情報とコンテンツＩＤとをタグとともにメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、コンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成る。

【００２０】この発明によるデータ配信システムにおいては、データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および／または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報と、コンテンツデータを特定するためのコンテンツＩＤとを取得し、そのコンテンツ情報およびコンテンツＩＤをタグとともにメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【００２１】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できるとともに、コンテンツメールを受取った他の端末装置のユーザはタグに基づいてコンテンツデータの配信をサーバへ要求することができる。その結果、ユーザの負荷を一層軽減できる。

【００２２】また、この発明によるデータ配信システムは、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとを保持するサーバと、サーバからコンテンツファイルおよびライセンスをダウンロードし、そのダウンロードしたコンテンツファイルおよびライセンスをデータ記録装置に記録および／または再生するとともに、コンテンツファイルに含まれるコンテンツ情報とコンテンツＩＤとをタグとともにメールに付加してコ

ンテンツメールを作成し、その作成したコンテンツメールを出力するデータ端末装置と、コンテンツメールを受信し、その受信したコンテンツメールに含まれるコンテンツＩＤをサーバへ送信してサーバからコンテンツＩＤによって特定されるコンテンツファイルをダウンロードする他の端末装置と、メールサーバからコンテンツメールを受信し、その受信したコンテンツメールを他の端末装置へ送信するメールサーバとから成る。

【００２３】この発明によるデータ配信システムにおいては、データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および／または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報と、コンテンツデータを特定するためのコンテンツＩＤとを取得し、そのコンテンツ情報およびコンテンツＩＤをタグとともにメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【００２４】そうすると、他の端末装置は、コンテンツメールを受信し、コンテンツメールに含まれるコンテンツＩＤをタグを手がかりにしてサーバへ送信してコンテンツＩＤによって特定されるコンテンツファイルをダウンロードする。

【００２５】したがって、この発明によれば、コンテンツメールを受信した他の端末装置のユーザは、コンテンツＩＤを取得しなくても、コンテンツファイルをダウンロードできる。

【００２６】好ましくは、データ端末装置は、他の端末装置からのコンテンツ情報の送信要求に応じてコンテンツメールを出力する。

【００２７】データ端末装置は、他の端末装置からのコンテンツ情報の送信要求を受信すると、コンテンツ情報を含むコンテンツメールを作成し、他の端末装置へコンテンツメールを送信する。

【００２８】したがって、この発明によれば、他のユーザからの要求に応じてコンテンツ情報を送信できる。その結果、他のユーザはサーバへアクセスしなくてもコンテンツ情報を容易に取得できる。

【００２９】好ましくは、データ端末装置は、ユーザによって入力されたコンテンツ情報の送信要求に応じてコンテンツメールを出力する。

【００３０】データ端末装置は、コンテンツ情報の送信要求が入力されると、コンテンツ情報を含むコンテンツメールを作成し、他の端末装置へコンテンツメールを送信する。

【００３１】したがって、この発明によれば、ユーザは自己の有するコンテンツデータに関するコンテンツ情報を他のユーザに知らせることができる。

【００３２】また、この発明によるデータ端末装置は、コンテンツデータをファイル形式によって保持するコンテンツファイルと、コンテンツファイルを利用するためのライセンスとをサーバからダウンロードしてデータ記録装置に記録し、コンテンツファイルに含まれるコンテンツ情報を他の端末装置へ送信するデータ端末装置であって、バスと、バスに接続され、データ記録装置とバスとの間でデータのやり取りを制御するインタフェースと、バスに接続され、外部と通信を行なう送受信部と、バスに接続され、情報を入力するためのキー操作部と、バスに接続され、他の端末装置へ送信するためのメールを作成するメール作成部と、バスに接続された制御部とを備え、コンテンツファイルのダウンロード時、制御部は、キー操作部から入力されたコンテンツファイルのダウンロード要求に応じて、コンテンツデータを特定するためのコンテンツＩＤをサーバへ送信するように送受信部を制御し、送受信部が受信したコンテンツファイルおよびライセンスをインタフェースを介してデータ記録装置へ出力し、送受信部は、制御部からの制御によりコンテンツＩＤをサーバへ送信し、コンテンツファイルおよびライセンスを受信し、コンテンツ情報の送信時、制御部は、コンテンツ情報の送信要求に応じて、インタフェースを介してデータ記録装置からコンテンツ情報を取得し、その取得したコンテンツ情報をメール作成部へ与え、メール作成部から出力されたコンテンツ情報を含むコンテンツメールを他の端末装置へ送信するように送受信部を制御し、メール作成部は、コンテンツ情報をメール文に付加したコンテンツメールを作成し、送受信部は、制御部からの制御によってコンテンツメールを他の装置へ送信する。

【００３３】データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録する。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報を取得し、そのコンテンツ情報をメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールを他の端末装置へ送信する。

【００３４】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できる。

【００３５】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、キー操作部から入力されたコンテンツ情報の送信要求に応じて、コンテンツ情報をデータ記録装置から取得する。

【００３６】データ端末装置においては、キー操作部からコンテンツ情報の送信要求に応じてコンテンツ情報を

データ記録装置から取得し、メール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールを他の端末装置へ送信する。

【００３７】したがって、この発明によれば、データ端末装置のユーザは、自己の有するコンテンツデータに関するコンテンツ情報を他のユーザに知らせることができる。

【００３８】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、送受信部が受信したコンテンツ情報の送信要求に応じて、コンテンツ情報をデータ記録装置から取得する。

【００３９】データ端末装置は、他の端末装置からのコンテンツ情報の送信要求を受信すると、コンテンツ情報を含むコンテンツメールを作成し、他の端末装置へコンテンツメールを送信する。

【００４０】したがって、この発明によれば、他のユーザからの要求に応じてコンテンツ情報を送信できる。その結果、他のユーザはサーバへアクセスしなくてもコンテンツ情報を容易に取得できる。

【００４１】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、インタフェースを介して複数のデータ記録装置からコンテンツ情報を取得し、メール作成部へ与える。

【００４２】データ端末装置は、複数のデータ記録装置に記録された全てのコンテンツデータに関するコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを他の端末装置へ送信する。

【００４３】したがって、この発明によれば、複数のデータ記録装置に記録されたコンテンツデータに関するコンテンツ情報を他の端末装置へ送信できる。

【００４４】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、インタフェースを介してユーザが保持する全てのデータ記録装置からコンテンツ情報を取得し、メール作成部へ与える。

【００４５】データ端末装置は、ユーザが保持する全てのコンテンツデータに関するコンテンツ情報をメール文に付加してコンテンツメールを作成し、その作成したコンテンツメールを他の端末装置へ送信する。

【００４６】したがって、この発明によれば、ユーザが保持する全てのコンテンツデータに関するコンテンツ情報を他の端末装置へ送信できる。

【００４７】好ましくは、コンテンツ情報の送信時、データ端末装置の制御部は、コンテンツ情報とともにコンテンツＩＤをインタフェースを介してデータ記録装置から取得し、コンテンツ情報およびコンテンツＩＤをメール作成部へ与え、メール作成部は、コンテンツ情報およびコンテンツＩＤをタグとともにメール文に付加してコンテンツメールを作成する。

【００４８】データ端末装置は、サーバからコンテンツデータを含むコンテンツファイルをダウンロードし、そのダウンロードしたコンテンツファイルをデータ記録装置に記録および／または再生を行なう。また、データ端末装置は、コンテンツファイルに含まれるコンテンツデータに関連するコンテンツ情報と、コンテンツデータを特定するためのコンテンツＩＤとを取得し、そのコンテンツ情報およびコンテンツＩＤをタグとともにメール文に付加してコンテンツメールを作成する。そして、データ端末装置は、作成したコンテンツメールをメールサーバを介して他の端末装置へ送信する。

【００４９】したがって、この発明によれば、データ端末装置は、自動的にコンテンツメールを作成し、他の端末装置へコンテンツメールを送信するので、表示機能や操作機能の乏しい端末装置におけるユーザの負荷を軽減できるとともに、コンテンツメールを受取った他の端末装置のユーザはタグに基づいてコンテンツデータの配信をサーバへ要求することができる。その結果、ユーザの負荷を一層軽減できる。

【００５０】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００５１】図１は、本発明によるデータ配信システムにおける暗号化コンテンツデータのメモリカードへの配信を概念的に説明するための概略図である。

【００５２】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば静止画、動画等の画像データ等を配信する場合においても適用することが可能なものである。

【００５３】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【００５４】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して、暗号化コンテンツデータとライ

センスとを配信する。

【００５５】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００５６】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００５７】以下では、このようなライセンスサーバ１０と配信キャリア２０とを併せて、配信サーバ３０と総称することにする。

【００５８】また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００５９】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００６０】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００６１】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００６２】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生装置（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００６３】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００６４】まず、配信サーバ３０より配信されるデータについて説明する。Ｄａｔａは、音楽データ等のコンテンツデータである。コンテンツデータＤａｔａには、ライセンスキーＫｃで復号可能な暗号化が施される。ライセンスキーＫｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

【００６５】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００６６】さらに、配信サーバ３０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、ライセンス情報としては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１および再生回路における制御情報である再生回路制御情報ＡＣ２等が存在する。以後、ライセンスキーＫｃとコンテンツＩＤとライセンスＩＤとアクセス制御情報ＡＣ１と再生回路制御情報ＡＣ２とを併せて、ライセンスと総称することとする。

【００６７】図３は、図１に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【００６８】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００６９】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。

【００７０】禁止クラスリストデータＣＲＬは、配信サーバ３０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データＣＲＬ＿ｄａｔを配信サーバ３０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬが書替えられる構成とする。また、禁止クラスリストのバージョンについては、ＣＲＬ＿ｖｅｒをメモリカード側より出力し、これを配信サーバ３０側

で確認することによってバージョン管理を実行する。差分データＣＲＬ＿ｄａｔには新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【００７１】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカード内でおいても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードへのライセンスキーの供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【００７２】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【００７３】コンテンツ再生回路（携帯電話機）およびメモリカードには固有の公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉがそれぞれ設けられ、公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉはコンテンツ再生回路に固有の秘密復号鍵Ｋｐｎおよびメモリカード固有の秘密復号鍵Ｋｍｃｉによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【００７４】また、コンテンツ再生回路およびメモリカードのクラス証明書として、ＣｒｔｆｎおよびＣｍｃｉがそれぞれ設けられる。

【００７５】これらのクラス証明書は、メモリカードおよびコンテンツ再生回路（携帯電話機）のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【００７６】これらのメモリカードおよびコンテンツ再生回路固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａおよび｛ＫＰｐｎ／／Ｃｒｔｆｎ｝ＫＰｍａの形式で、出荷時にメモリカードおよび携帯電話機のコンテンツ再生回路にそれぞれ記録される。後ほど詳細に説明するが、ＫＰｍａは配信システム全体で共通の公開認証鍵である。

【００７７】図４は、図１に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【００７８】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ３０、携帯電話機１００、メモリカード１１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００７９】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００８０】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００８１】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍと、公開暗号鍵ＫＰｍで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍが存在する。

【００８２】図５は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。

【００８３】ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４、課金データベース３０２およびＣＲＬデータベース３０６からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００８４】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生す

るためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを通信装置３５０およびバスＢＳ１を介して受けて、公開認証鍵ＫＰｍａによる復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｍを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００８５】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンスキーＫｃおよび再生回路制御情報ＡＣ２を、復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【００８６】ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００８７】図６は、図５に示す情報データベース３０４に保持されるコンテンツファイルを示したものである。情報データベース３０４は、複数の記録媒体４０を有する。記録媒体４０は、コンテンツファイル（Ｃｏｎｔｅｎｔ　Ｆｉｌｅ）１～コンテンツファイル５等の複数のコンテンツファイル４１を含む。

【００８８】図７は、記録媒体４０に含まれるコンテンツファイル４１の構成を示したものである。コンテンツファイル４１は、ファイルヘッダ（Ｆｉｌｅ　Ｈｅａｄｅｒ）４１０、コンテンツ情報（Ｃｏｎｔｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ）４２０、コンテンツテーブル（Ｔａｂｌｅ　ｏｆ　Ｄａｔａ　Ｏｂｊｅｃｔｓ）４３０、およびコンテンツデータ（Ｄａｔａ　Ｏｂｊｅｃｔｓ）１（４４０）～コンテンツデータＮ（４４ｎ）から成る。コンテンツデータ４４０～４４ｎの各々は、ライセンスキーＫｃによって復号可能なように暗号化されている。

【００８９】ファイルヘッダ４１０は、コンテンツを配信する配信プロトコルの固有識別情報であるＵＤＡＣＣｏｄｅ４１１と、プロトコルのバージョン番号を示すＰｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ４１２と、コンテンツの固有識別子であるＣｏｎｔｅｎｔＩＤ４１３と、コンテンツのバージョン番号を示すＣｏｎｔｅｎｔ　Ｖｅｒｓｉｏｎ４１４と、ファイルのバイトサイズを示すＦｉｌｅ　Ｌｅｎｇｔｈ４１５と、コンテンツの種類を示すＣｏｎｔｅｎｔ　Ｔｙｐｅ４１６と、コンテンツの再生時間を示すＰｌａｙ　Ｔｉｍｅ４１７と、コンテンツデータの数を示すＮｕｍｂｅｒ　ｏｆ　Ｄａｔａ　Ｏｂｊｅｃｔｓ４１８と、コンテンツ情報４２０のバイトサイズを示すＩｎｆｏｒｍａｔｉｏｎ　Ｌｅｎｇｔｈ４１９とから構成される。

【００９０】また、コンテンツ情報４２０は、曲名４２１およびアーティスト名４２２とから構成され、コンテンツデータ４４０～４４ｎに関連する情報が含まれる。コンテンツテーブル４３０は、コンテンツデータ４４０～４４ｎの各々のファイル上の位置やサイズ情報である。コンテンツデータ４４０～４４ｎは、コンテンツの実体である音楽や歌詞データである。図７に示すファイル構成によって１つのコンテンツファイルが構成される。また、コンテンツデータ４４０～４４ｎによって１つのコンテンツデータが構成される。つまり、コンテンツデータ４４０～４４ｎによって１つのコンテンツデータ｛Ｄａｔａ｝Ｋｃを構成する。したがって、携帯電話機１００のユーザからコンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求があったときは、そのコンテンツデータ｛Ｄａｔａ｝Ｋｃが含まれるコンテンツファイルが携帯電話機１００に配信される。

【００９１】図８は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【００９２】携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのバスＢＳ２と、バスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

【００９３】携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのキー操作部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データベースＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを含む。ここで、携帯電話機（コンテンツ再生回路）１００のクラスｎは、ｎ＝１であるとする。

【００９４】携帯電話機１００は、さらに、音声再生部１１１２の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１１１３と、ＤＡ変換器１１１３の出力を外部出力装置等へ出力するための端子１１１４とを含む。

【００９５】携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００と

を含む。

【００９６】携帯電話機１００は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｒｔｆ１を公開復号鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを保持する認証データ保持部１２０２を含む。

【００９７】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１２０４と、バスＢＳ２から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１２０６とを含む。

【００９８】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１２１０と、生成されたセッションキーＫｓ３を復号処理部１２０６によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ２に出力する暗号化処理部１２０８とを含む。

【００９９】携帯電話機１００は、さらに、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１２１２とを含む。

【０１００】携帯電話機１００は、さらに、バスＢＳ２より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１２１２より取得したライセンスキーＫｃによって復号しコンテンツデータを出力する復号処理部１２１４と、復号処理部１２１４の出力を受けてコンテンツデータを再生するための音楽再生部１２１６と、音楽再生部１２１６の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１２１８と、ＤＡ変換器１１１３とＤＡ変換器１２１８との出力を受けて、動作モードに応じて選択的に端子１１１４または端子１２２０から出力するためのスイッチ１２２２と、スイッチ１２２２の出力を受けて、ヘッドホーン１３０と接続するための接続端子１２２４とを含む。

【０１０１】携帯電話機１００は、さらに、配信サーバ１０から配信されたコンテンツデータのコンテンツ情報４２０をメール文に付加してコンテンツメールを作成するメール作成部１２２６を含む。

【０１０２】なお、図８においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生と、コンテンツメールの作成とにかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１０３】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１０４】図９は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃｉおよびＫｍｃｉが設けられ、メモリカードのクラス証明書Ｃｍｃｉが設けられるが、メモリカード１１０においては、これらは自然数ｉ＝１でそれぞれ表わされるものとする。

【０１０５】したがって、メモリカード１１０は、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ１を保持するＫｍｃ保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Ｋｍ１を保持するＫｍ１保持部１４２１と、Ｋｍ１によって復号可能な公開暗号鍵ＫＰｍ１を保持するＫＰｍ１保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵ＫＰｍｃ１およびクラス証明書Ｃｍｃ１を公開認証鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａとして保持する。

【０１０６】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

【０１０７】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０１を介して授受するバスＢＳ３と、バスＢＳ３にメモリインタフェース１２００から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵ＫｍｃｌをＫｍｃ１保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４０４と、ＫＰｍａ保持部１４１４から認証鍵ＫＰｍａを受けて、バスＢＳ３に与えられるデータからＫＰｍａによる復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号化処理部１４０６とを含む。

【０１０８】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｎもしくはＫＰｍｃｉによって暗号化してバスＢＳ３に送出する暗号化処理部１４１０と、バスＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキ

ーＫｓ２によって復号し、復号結果をバスＢＳ４に送出する復号処理部１４１２とを含む。

【０１０９】メモリカード１１０は、さらに、バスＢＳ３上のデータを公開暗号鍵ＫＰｍ１と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号するための復号処理部１４２２と、公開暗号鍵ＫＰｍ１で暗号化されている、ライセンスキーＫｃ、再生回路制御情報ＡＣ２および再生情報（コンテンツＩＤ，ライセンスＩＤ，アクセス制御情報ＡＣ１）と、暗号化されていない禁止クラスリストのバージョン更新のための差分データＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬとをバスＢＳ４より受けて格納するとともに、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。

【０１１０】メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を保持するためのライセンス情報保持部１４４０と、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１１１】ライセンス情報保持部１４４０は、バスＢＳ４との間でライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１のデータの授受が可能である。ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

【０１１２】なお、図９において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）である。

【０１１３】もちろん、メモリ１４１５も含めて、モジュールＴＲＭ内に組込まれる構成としてもよい。しかしながら、図９に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

【０１１４】次に、図１に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【０１１５】図１０および図１１は、図１に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１および第２のフローチャートである。

【０１１６】図１０および図１１においては、携帯電話ユーザが、メモリカード１１０を用いることで、携帯電話機１００を介して配信サーバ３０から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【０１１７】まず、携帯電話ユーザの携帯電話機１００から、携帯電話ユーザによるキー操作部１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【０１１８】メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａが出力される（ステップＳ１０２）。

【０１１９】携帯電話機１００は、メモリカード１１０からの認証のための認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

【０１２０】配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａ、ライセンス購入条件のデータＡＣを受信し（ステップＳ１０６）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰｍａで復号処理を実行する（ステップＳ１０８）。

【０１２１】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍｃ１と証明書Ｃｍｃ１を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１０）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を承認し、受理する。そして、次の処理（ステップＳ１１２）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を受理しないで処理を終了する（ステップＳ１７０）。

【０１２２】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍｃ１が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

【０１２３】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

【０１２４】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ１によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

【０１２５】暗号化されたセッションキーＫｓ１は、｛Ｋｓ１｝Ｋｍｃ１として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

【０１２６】携帯電話機１００が、暗号化されたセッションキー｛Ｋｓ１｝Ｋｍｃ１を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、バスＢＳ３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ１により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１２０）。

【０１２７】コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

【０１２８】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストの状態（バージョン）に関連する情報として、リストのバージョンデータＣＲＬ＿ｖｅｒをメモリ１４１５から抽出してバスＢＳ４に出力する。

【０１２９】暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍ１および禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１２２）。

【０１３０】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１は、バスＢＳ３から端子１２０１およびメモリインタフェース１２００を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

【０１３１】配信サーバ３０は、暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍ１およびメモリカード１１０における禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを受理する（ステップＳ１２６）。

【０１３２】禁止クラスリストのバージョン情報ＣＲＬ＿ｖｅｒは、バスＢＳ１を介して配信制御部３１５に送られ、配信制御部３１５は、受理したバージョンデータＣＲＬ＿ｖｅｒに従って、当該ＣＲＬ＿ｖｅｒのバージョンとＣＲＬデータベース３０６内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データＣＲＬ＿ｄａｔを生成する（ステップＳ１２８）。

【０１３３】さらに、配線制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件データＡＣに従って、ライセンスＩＤ、アクセス制限情報ＡＣ１および再生回路制御情報ＡＣ２を生成する（ステップＳ１３０）。さらに、暗号化コンテンツデータを復号するためのライセンスキーＫｃを情報データベース３０４より取得する（ステップＳ１３２）。

【０１３４】図１１を参照して、配信制御部３１５は、生成したライセンス、すなわち、ライセンスキーＫｃ、再生回路制御情報ＡＣ２、ライセンスＩＤ、コンテンツＩＤ、およびアクセス制限情報ＡＣ１を暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ１によってライセンスを暗号化する（ステップＳ１３６）。暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの差分データＣＲＬ＿ｄａｔとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、バスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

【０１３５】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１３６】携帯電話機１００は、送信された暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ２を受信し（ステップＳ１４０）、メモリインタフェース１２００を介してメモリカード１１０へ出力する。メモリカード１１０においては、メモリインタフェース１

２００を介して、バスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ３の受信データを復号しバスＢＳ４に出力する（ステップＳ１４２）。

【０１３７】この段階で、バスＢＳ４には、Ｋｍ１保持部１４２１に保持される秘密復号鍵Ｋｍ１で復号可能な暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１と、ＣＲＬ＿ｄａｔとが出力される。コントローラ１４２０の指示によって、暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１は、メモリ１４１５に記録される（ステップＳ１４４）。一方、暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１は、復号処理部１４２２において、秘密復号鍵Ｋｍ１によって復号され、ライセンスのうち、メモリカード１１０内で参照されるライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１のみが受理される（ステップＳ１４６）。

【０１３８】コントローラ１４２０は、受理したＣＲＬ＿ｄａｔに基づいて、メモリ１４１５内の禁止クラスリストデータＣＲＬおよびそのバージョンを更新する（ステップＳ１４８）。さらに、ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１については、ライセンス情報保持部１４４０に記録される（ステップＳ１５０）。

【０１３９】ステップＳ１５０までの処理がメモリ回路で正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ１５２）。

【０１４０】配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１５４）。この場合、配信サーバ３０は、情報データベース３０４の記録媒体４０からファイルヘッダ４１０、コンテンツ情報４２０、およびデータテーブル４３０を付加情報Ｄａｔａ－ｉｎｆとして取得する。つまり、配信サーバ３０は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃが含まれる１つのコンテンツファイル［Ｄａｔａ－ｉｎｆ（ファイルヘッダ４１０＋コンテンツ情報４２０＋データテーブル４３０）／／｛Ｄａｔａ｝Ｋｃ（コンテンツデータ４４０～４４ｎ）］を取得する。

【０１４１】携帯電話機１００は、Ｄａｔａ－ｉｎｆ／／｛Ｄａｔａ｝Ｋｃを受信して、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを受理する（ステップＳ１５６）。暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆは、メモリインタフェース１２００および端子１２０１を介してメモリカード１１０のバスＢＳ３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆがそのままメモリ１４１５に記録される（ステップＳ１５８）。つまり、図７に示すファイル構成によって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆがメモリ１４１５に記録される。

【０１４２】さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ１６０）、配信サーバ３０で配信受理を受信すると（ステップＳ１６２）、課金データベース３０２への課金データの格納等を伴って、配信終了の処理が実行され（ステップＳ１６４）、全体の処理が終了する（ステップＳ１７０）。

【０１４３】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍｃ１とともに暗号化して送信できた公開暗号鍵ＫｐｌおよびＫｍｃ１が有効であることを確認した上で、それぞれのクラス証明書Ｃｍｃ１が禁止クラスリスト、すなわち、公開暗号鍵ＫｐｌおよびＫｍｃ１による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１４４】次に、図１２および図１３を参照してメモリカード１１０に配信されたコンテンツデータの携帯電話機１００における再生動作について説明する。図１２を参照して、再生動作の開始とともに、携帯電話機１００のユーザからキー操作部１１０８を介して再生指示が携帯電話機１００にインプットされる（ステップＳ２００）。そうすると、コントローラ１１０６は、バスＢＳ２を介して認証データ保持部１２０２から認証データ｛ＫＰｐｌ／／Ｃｒｔｆ１｝ＫＰｍａを読出し、メモリインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを入力する（ステップＳ２０１）。

【０１４５】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを受理する（ステップＳ２０２）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを、ＫＰｍａ保持部１４１４に保持された公開認証鍵ＫＰｍａによって復号し（ステップＳ２０３）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ２０４）。復号できなかった場合、コントローラ１４２０は認証データ不受理の出力を

データＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２０６）。認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｒｔｆ１がメモリ１４１５から読出した禁止クラスリストデータに含まれるか否かを判断する（ステップＳ２０５）。この場合、証明書Ｃｒｔｆ１にはＩＤが付与されており、コントローラ１４２０は、受理した証明書Ｃｒｔｆ１のＩＤが禁止クラスリストデータの中に存在するか否かを判別する。証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれると判断されると、コントローラ１４２０は認証データ不受理の出力をデータＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２０６）。

【０１４６】ステップＳ２０４において認証データが公開認証鍵ＫＰｍａで復号できなかったとき、およびステップＳ２０５において受理した証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ１１１０に表示する（ステップＳ２０７）。

【０１４７】ステップＳ２０５において、証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれていないと判断されると、図１３を参照して、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ２０８）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ２０９）。そうすると、コントローラ１４２０は、端子１２０１を介してメモリインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力し、携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１２０４は、秘密復号鍵Ｋｐ１を復号処理部１２０６へ出力する。

【０１４８】復号処理部１２０６は、Ｋｐ１保持部１２０４から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１２０８へ出力する（ステップＳ２１０）。そうすると、セッションキー発生部１２１０は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１２０８へ出力する（ステップＳ２１１）。暗号処理部１２０８は、セッションキー発生部１２１０からのセッションキーＫｓ３を復号処理部１２０６からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、バスＢＳ２およびメモリインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ２１２）。

【０１４９】メモリカード１１０の復号処理部１４１２は、端子１２０１およびバスＢＳ３を介して｛Ｋｓ３｝Ｋｓ２を入力し、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、携帯電話機１００で発生されたセッションキーＫｓ３を取得する（ステップＳ２１３）。

【０１５０】セッションキーＫｓ３の受理に応じて、コントローラ１４２０は、ライセンス情報保持部１４４０内の対応するアクセス制限情報ＡＣ１を確認する（ステップＳ２１４）。

【０１５１】ステップＳ２１４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数に制限がある場合にはアクセス制限情報ＡＣ１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ２１５）。一方、アクセス制限情報ＡＣ１によって再生回数が制限されていない場合においては、ステップＳ２１５はスキップされ、アクセス制御情報ＡＣ１は更新されることなく処理が次のステップ（ステップＳ２１６）に進行される。

【０１５２】また、ライセンス情報保持部１４４０内にリクエスト曲の当該コンテンツＩＤが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【０１５３】ステップＳ２１４において、当該再生動作において再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキーＫｃを含むライセンスの復号処理が実行される。具体的には、コントローラ１４２０の指示に応じて、メモリ１４１５からバスＢＳ４に読出された暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１を復号処理部１４２２がメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号し、再生処理に必要なライセンスキーＫｃと再生回路制御情報ＡＣ２がバスＢＳ４上に得られる（ステップＳ２１６）。

【０１５４】得られたライセンスキーＫｃと再生回路制御情報ＡＣ２は、切換スイッチ１４４４の接点Ｐｄを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｄを介して復号処理部１４１２より受けたセッションキーＫｓ３によってバスＢＳ４から受けたライセンスキーＫｃと再生回路制御情報ＡＣ２とを暗号化し、｛Ｋｃ／／ＡＣ２｝Ｋｓ３をバスＢＳ３に出力する（ステップＳ２１７）。

【０１５５】バスＢＳ３に出力された暗号化データは、メモリインタフェース１２００を介して携帯電話機１０

０に送出される。

【０１５６】携帯電話機１００においては、メモリインタフェース１２００を介してバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｓ３を復号処理部１２１２によって復号処理を行ない、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２を受理する（ステップＳ２１８）。復号処理部１２１２は、ライセンスキーＫｃを復号処理部１２１４に伝達し、再生回路制御情報ＡＣ２をバスＢＳ２に出力する。

【０１５７】コントローラ１１０６は、バスＢＳ２を介して、再生回路制御情報ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２１９）。

【０１５８】ステップＳ２１９においては、再生回路制御情報ＡＣ２によって再生不可と判断される場合には、再生動作は終了される。

【０１５９】ステップＳ２１９において再生可能と判断された場合、コントローラ１１０６は、メモリインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ３および端子１２０１を介してメモリインタフェース１２００へ出力する（ステップＳ２２０）。

【０１６０】携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１４へ与える。そして、復号処理部１２１４は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１２から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ２２１）。

【０１６１】そして、復号されたコンテンツデータＤａｔａは音楽再生部１２１６へ出力され、音楽再生部１２１６は、コンテンツデータを再生し、ＤＡ変換器１２１８はディジタル信号をアナログ信号に変換して端子１２２０へ出力する。そして、スイッチ１２２２は端子１２２０を選択して音楽データは端子１２２４を介してヘッドホーン１３０へ出力されて再生される（ステップＳ２２２）。これによって再生動作が終了する。

【０１６２】上述したように、携帯電話機１００のユーザは、携帯電話機１００を用いて配信サーバ３０から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをメモリカード１１０に受信し、ライセンスキーＫｃによって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号して再生することができる。

【０１６３】本発明においては、携帯電話機１００は、配信サーバ３０から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをメモリカード１１０に受信した後、携帯電話機１００のユーザからの要求に応じて暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのコンテンツ情報をメールに付加してコンテンツメールを作成し、その作成したコンテンツメールを他の携帯電話機に送信する。すなわち、図１４を参照して、携帯電話機１００は、携帯電話網２０、およびメールサーバ１５０を介して携帯電話機１２０とメールのやり取りを行なう。

【０１６４】携帯電話機１２０は、図８に示す携帯電話機１００の構成と同じ構成から成る。また、携帯電話機１２０には、メモリカード１４０が脱着可能であり、メモリカード１４０は図９に示すメモリカード１１０の構成と同じ構成から成る。携帯電話機１００は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのアーティスト名および曲名をメモリカード１１０から取得し、アーティスト名および曲名をメールに付加することによってコンテンツメールを作成する。そして、携帯電話機１００は、作成したコンテンツメールを携帯電話機１２０へ送信するために携帯電話網２０へ出力する。携帯電話機網２０は、コンテンツメールをメールサーバ１５０へ送信し、メールサーバ１５０はコンテンツメールのヘッダ部に付けられたアドレスから携帯電話機１２０を特定する。そして、メールサーバ１５０は、特定した携帯電話機１２０へコンテンツメールを送信する。携帯電話機１２０は、コンテンツメールを受取り、その受取ったアーティスト名および曲名をディスプレイ１１１０に表示する。これにより、携帯電話機１２０のユーザは、携帯電話機１００に装着されたメモリカード１１０に聴きたい音楽データが記録されているかどうかを知ることができる。

【０１６５】そして、携帯電話機１２０のユーザは、受信したコンテンツメールをディスプレイ１１１０に表示し、取得した暗号化コンテンツデータがあれば、配信サーバ３０へ暗号化コンテンツデータの配信を要求する。そして、携帯電話機１２０は、受信した暗号化コンテンツデータと、その暗号化コンテンツデータを復号するためのライセンスキーとを装着されたメモリカード１４０へ記録および／または再生を行なう。

【０１６６】図１５を参照して、携帯電話機１００が携帯電話網２０を介して携帯電話機１２０へコンテンツ情報をメールに付加したコンテンツメールを送信する動作について説明する。携帯電話機１００のユーザからキー操作部１１０８を介してコンテンツ情報の配信要求が入力されると（Ｓ３００）、コントローラ１１０６は、メモリインタフェース１２００を介してメモリカード１１０のメモリ１４１５に記録されたファイルヘッダ４１０の読出しを要求する。メモリカード１１０のコントローラ１４２０は、端子１２０１、およびバスＢＳ３を介してファイルヘッダ４１０の読出要求を受取り、メモリ１４１５からファイルヘッダ４１０を読出す。この場合、コントローラ１４２０は、メモリカード１１０上に構築されたファイルシステムの管理情報を参照してファイル

ヘッダ４１０を読出す。そして、コントローラ１４２０は、バスＢＳ３および端子１２０１を介して読出したファイルヘッダ４１０をメモリインタフェース１２００へ出力する。そして、コントローラ１１０６は、ファイルヘッダ４１０を受取る（ステップＳ３０２）。なお、アーティスト名および曲名は、コンテンツファイルのコンテンツ情報４２０に含まれるから、最初からコンテンツ情報４２０を読出すのが普通であるが、図７に示すファイル構成においては、ファイルヘッダ４１０を読出さなければ、コンテンツ情報４２０を読出すことができない構成になっている。

【０１６７】携帯電話機１００のコントローラ１１０６は、ファイルヘッダ４１０を読出した後、コンテンツ情報４２０の読出要求をメモリインタフェース１２００を介してメモリカード１１０へ出力する。そうすると、メモリカード１１０のコントローラ１４２０は、端子１２０１およびバスＢＳ３を介してコンテンツ情報４２０の読出要求を受取り、メモリカード１１０上に構築されたファイルシステムの管理情報を参照しながらメモリ１４１５からコンテンツ情報４２０を読出す。そして、コントローラ１４２０は、バスＢＳ３および端子１２０１を介してメモリインタフェース１２００にコンテンツ情報４２０を出力する。携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介してコンテンツ情報４２０を受取り、バスＢＳ２を介してコンテンツ情報４２０をメール作成部１２２６へ出力する。

【０１６８】メール作成部１２２６は、コンテンツ情報４２０をバスＢＳ２を介して受取り、コンテンツ情報４２０であるアーティスト名および曲名を、字間、字体等を整えながらメール本体に付加してコンテンツメールを作成し、コンテンツメールを出力する（ステップＳ３０４）。コントローラ１１０６は、メモリカード１１０に記録された全てのファイルヘッダを読出したか否かを判断する（ステップＳ３０６）。メモリカード１１０に記録された全てのファイルヘッダ４１０が読出されていないとき、ステップＳ３０２，Ｓ３０４，Ｓ３０６が繰返される。そして、コンテンツメールに次々とコンテンツ情報４２０が追加される。

【０１６９】メモリカード１１０から全てのファイルヘッダ４１０が読出されたと判断されると、次に、コントローラ１１０６は、他のメモリカードについても処理するか否かを判断する（ステップＳ３０８）。他のメモリカードも処理する場合、ステップＳ３０２，Ｓ３０４，Ｓ３０６，Ｓ３０８が繰返される。つまり、ステップＳ３０２，Ｓ３０４，Ｓ３０６，Ｓ３０８は、携帯電話機１００のユーザが所有するメモリカードに含まれる全てのコンテンツ情報４２０を他の携帯電話機１２０へ送信するためのステップである。そして、コントローラ１１０６は、他のメモリカードは処理しないと判断すると、メール作成部１２２６から出力されたコンテンツメールをバスＢＳ２を介して受取り、送受信部１１０４へコンテンツメールを出力する。そして、送受信部１１０４は、アンテナ１１０２を介してコンテンツメールを送信し、携帯電話網２０はコンテンツメールをメールサーバ１５０へ送る。メールサーバ１５０は、コンテンツメールのアドレスに基づいて携帯電話機１２０を特定し、携帯電話網２０を介してコンテンツメールを携帯電話機１２０へ送信する（ステップＳ３１０）。これによってメールの送信動作が終了する（ステップＳ３１２）。

【０１７０】コンテンツメールを受取った携帯電話機１２０のユーザは、携帯電話機１２０のディスプレイ１１１０に表示されたアーティストおよび曲名を見てダウンロードしたい暗号化コンテンツデータがあれば、配信サーバ３０に対して希望する暗号化コンテンツデータの配信要求を行なう。携帯電話機１２０が配信サーバ３０から暗号化コンテンツデータをダウンロードする動作は、図１０および図１１に示すフローチャートに従って行なわれる。

【０１７１】メモリカード１１０に記録された暗号化コンテンツデータのコンテンツ情報４２０を自動的に作成し、その作成したコンテンツメールを携帯電話機１００から携帯電話機１２０へ送信することによって、表示機能や操作機能が貧弱な携帯電話機におけるユーザの負荷を軽減することができる。

【０１７２】本発明による暗号化コンテンツデータのコンテンツ情報４２０を他の携帯電話機へメールによって送信する動作は、図１６に示すフローチャートに従って行なっても良い。図１６に示すフローチャートは、図１５に示すフローチャートのステップＳ３０４をステップＳ３０３に代え、かつ、その代えたステップＳ３０３とステップＳ３０６との間にステップＳ３０５を挿入したものであり、その他は図１５に示すフローチャートと同じである。携帯電話機１００のコントローラ１１０６は、メモリカード１１０からコンテンツ情報４２０を読出し、そのコンテンツ情報をメール作成部１２２６へ与えると、メール作成部１２２６は、タグとともにコンテンツ情報４２０をメール本体に付加してコンテンツメールを作成する（ステップＳ３０３）。

【０１７３】そして、コントローラ１１０６は、既にメモリカード１１０から読出したファイルヘッダ４１０に含まれるコンテンツＩＤを抽出し、コンテンツＩＤをメール作成部１２２６に与える。メール作成部１２２６は、受取ったコンテンツＩＤを字間、字体等を調整してメール本体に付加する（ステップＳ３０５）。

【０１７４】ここで、「タグ」とは、ユーザがコンテンツメールを見て、そのコンテンツメールの情報を対象として操作を行なえるようにするための制御信号である。タグの利用方法としては、コンテンツメールを受信した携帯電話機１２０のユーザが携帯電話機１００のユーザと同じコンテンツファイル（暗号化コンテンツデータ）

のダウンロードを希望する場合、コンテンツメールからタグを参照し、コンテンツＩＤを抽出することによって、暗号化コンテンツデータのダウンロード時にコンテンツＩＤを取得する過程を省略することが考えられる。その後、図１５に示すステップＳ３０６，Ｓ３０８，Ｓ３１０，Ｓ３１２と同じ動作が行なわれてコンテンツメールの携帯電話機１００から携帯電話機１２０への送信は終了する。

【０１７５】コンテンツ情報に加え、タグとともにコンテンツＩＤを付加して作成したコンテンツメールを送信する場合、表示機能や操作機能の貧弱な携帯電話機におけるユーザの負荷を軽減できるとともに、ユーザがコンテンツファイル（暗号化コンテンツデータ）、およびそのライセンスを配信サーバからダウンロードする際に必要となるコンテンツＩＤの取得処理を軽減することができる。

【０１７６】また、上記においては、携帯電話機１００のユーザがキー操作部１１０８からコンテンツ情報のメールによる送信を要求する場合について説明したが、本発明は、かかる場合に限られず、携帯電話機１２０のユーザが携帯電話機１００へコンテンツ情報の送信を要求し、携帯電話機１００がコンテンツ情報を携帯電話機１２０へ送信する場合であっても良い。この場合、携帯電話機１００のコントローラ１１０６は、送受信部１１０４からコンテンツ情報の送信要求を受取ると、図１５または図１６に示すフローチャートに従ってコンテンツメールを作成し、その作成したコンテンツメールを携帯電話機１２０へ送信する。こうにすることによって、携帯電話機のユーザ間においてコンテンツ情報を自由にやり取りすることができ、ユーザの負荷を一層軽減できる。

【０１７７】なお、上記においては、暗号化コンテンツデータを対象として説明したが、本発明は暗号化コンテンツデータに限らず、暗号化されていないコンテンツデータも対象とする。また、携帯電話機を例にして暗号化コンテンツデータの配信、再生、およびコンテンツ情報のメールについて説明したが、本発明は携帯電話機に限らず、他の携帯端末装置であっても良い。

【０１７８】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

【図５】　ライセンスサーバの構成を示す概略ブロック図である。

【図６】　図５に示すライセンスサーバの情報データベースの構成図である。

【図７】　コンテンツファイルの構成図である。

【図８】　携帯電話機の構成を示すブロック図である。

【図９】　メモリカードの構成を示すブロック図である。

【図１０】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図１１】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１２】　携帯電話機における再生動作を説明するための第１のフローチャートである。

【図１３】　携帯電話機における再生動作を説明するための第２のフローチャートである。

【図１４】　コンテンツメールを送信するシステムを概念的に説明する概略ブロック図である。

【図１５】　図１４に示すシステムにおいてコンテンツメールの送信動作を説明するフローチャートである。

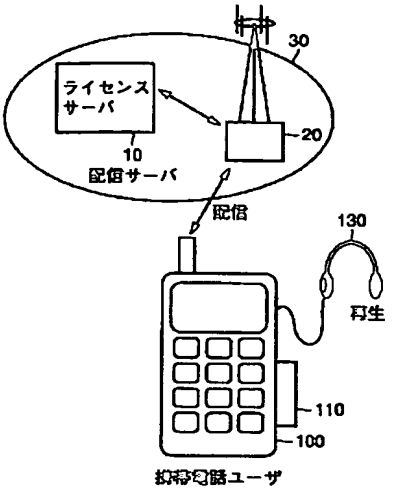
【図１６】　図１４に示すシステムにおいてコンテンツメールの送信動作を説明する他のフローチャートである。

【符号の説明】

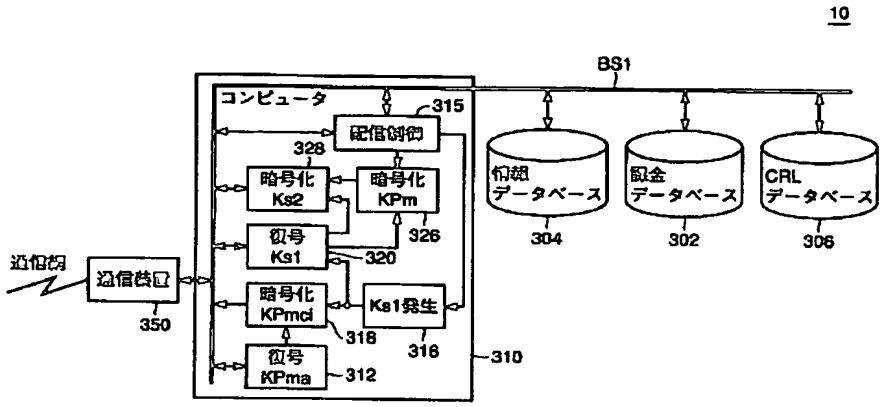
１０　ライセンスサーバ、２０　配信キャリア、３０　配信サーバ、４０　記録媒体、４１　コンテンツファイル、４１０　ファイルヘッダ、４１１　UDAC Code、４１２　プロトコルバージョン、４１３　コンテンツＩＤ、４１４　コンテンツバージョン、４１５　ファイル長、４１６　ContentType、４１７　Play Time、４１８　Number of Data Objects、４１９　Information Length、４２０コンテンツ情報、４２１　曲名、４２２　アーティスト名、４３０　データテーブル、４４０～４４ｎ　コンテンツデータ、１００，１２０　携帯電話機、１１０，１４０　メモリカード、１３０　ヘッドホーン、１１０６，１４２０　コントローラ、３０２　課金データベース、３０４　情報データベース、３０６ＣＲＬデータベース、３１０　データ処理部、３１２，３２０，１２０６，１２１２，１２１４，１４０４，１４０６，１４０８，１４１２，１４２２　復号処理部、３１５　配信制御部、３１６，１２１０，１４１８　セッションキー発生部、３１８，３２６，３２８，１２０８，１４１０　暗号処理部、３５０　通信装置、１１０２　アンテナ、１１０４　送受信部、１１０８　キー操作部、１１１０　ディスプレイ、１１１２　音声再生部、１１１３，１２１８　ＤＡ変換器、１１

１４，１２０１，１２２０，１２２４　端子、１２００　メモリインタフェース、１２０２，１４００　認証データ保持部、１２０４　Ｋｐ１保持部、１２１６　音楽再生部、１２２２　スイッチ、１２２６　メール作成部、１４０２Ｋｍｃ１保持部、１４１４　ＫＰｍａ保持部、１４１５　メモリ、１４１６ＫＰｍ１保持部、１４２１　Ｋｍ１保持部、１４４０　ライセンス情報保持部、１４４２，１４４４，１４４６　切換スイッチ。

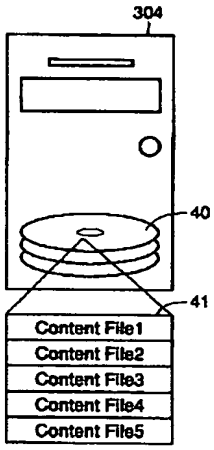
【図１】



【図５】



【図６】



【図２】

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
(Data)Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可）
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話)における制御情報（例：再生可否）

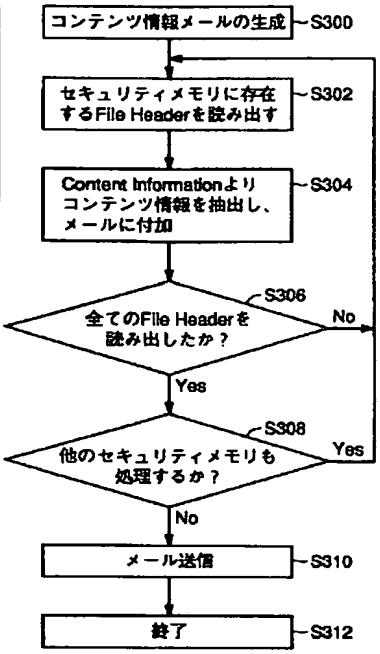
【図４】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵（非対称鍵）	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

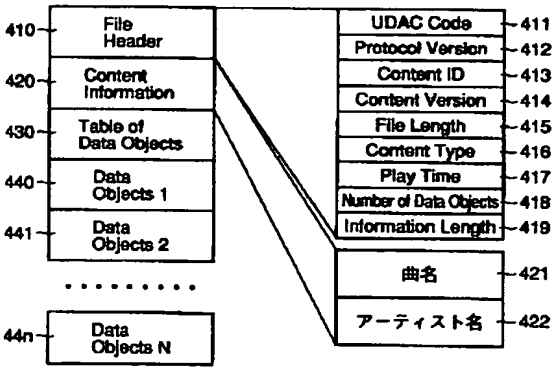
【図３】

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 （差分データ形式）
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 （非対称鍵）	携帯電話機	Kpnにて復号可能。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機の種類nごとに異なる。
KPmcl	公開暗号鍵 （非対称鍵）	メモリカード	Kmclにて復号可能。 {KPmcl//Cmcl}KPmaの形式で出荷時に記録 ＊メモリカードの種類lごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路（携帯電話機）固有の復号鍵 ＊携帯電話機の種類nごとに異なる。
Kmcl	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ＊メモリカードの種類lごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機のクラスnごとに異なる。
Cmcl		メモリカード	メモリカードのクラス証明書。認証機能を有する。 {KPmcl//Cmcl}KPmaの形式で出荷時に記録 ＊メモリカードのクラスlごとに異なる。

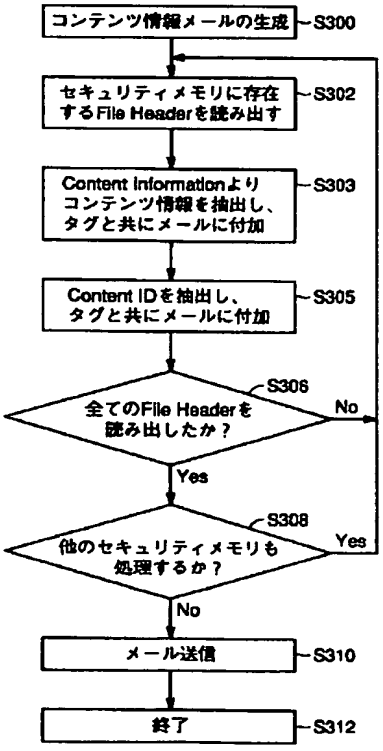
【図１５】



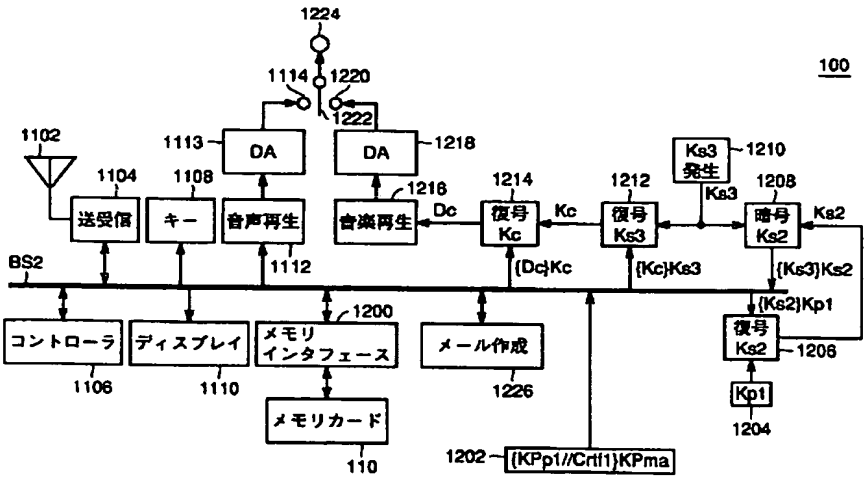
【図７】



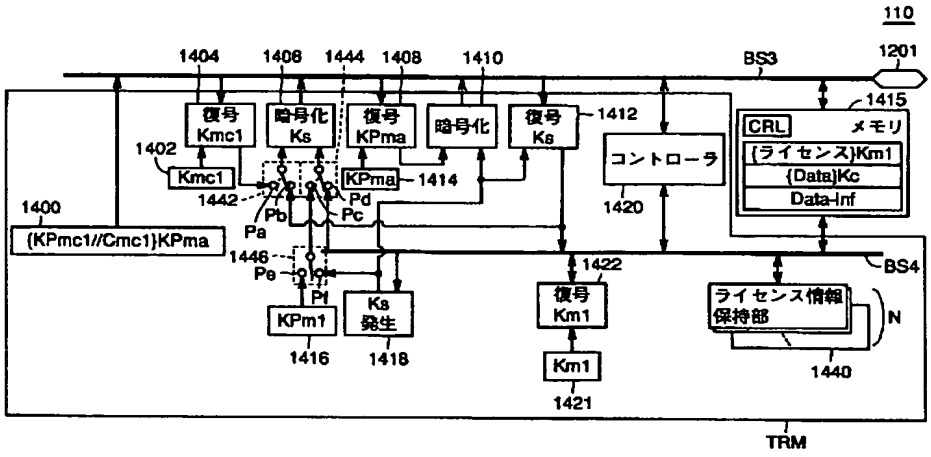
【図１６】



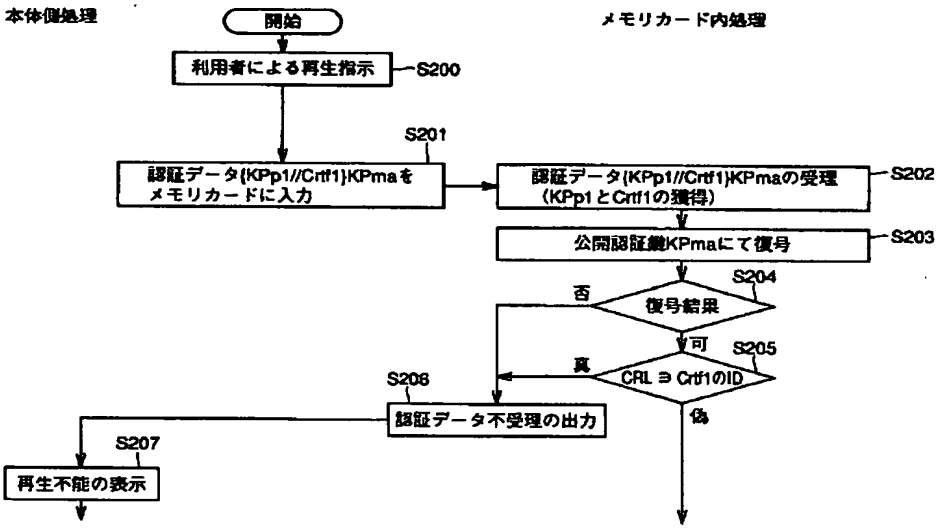
【図８】



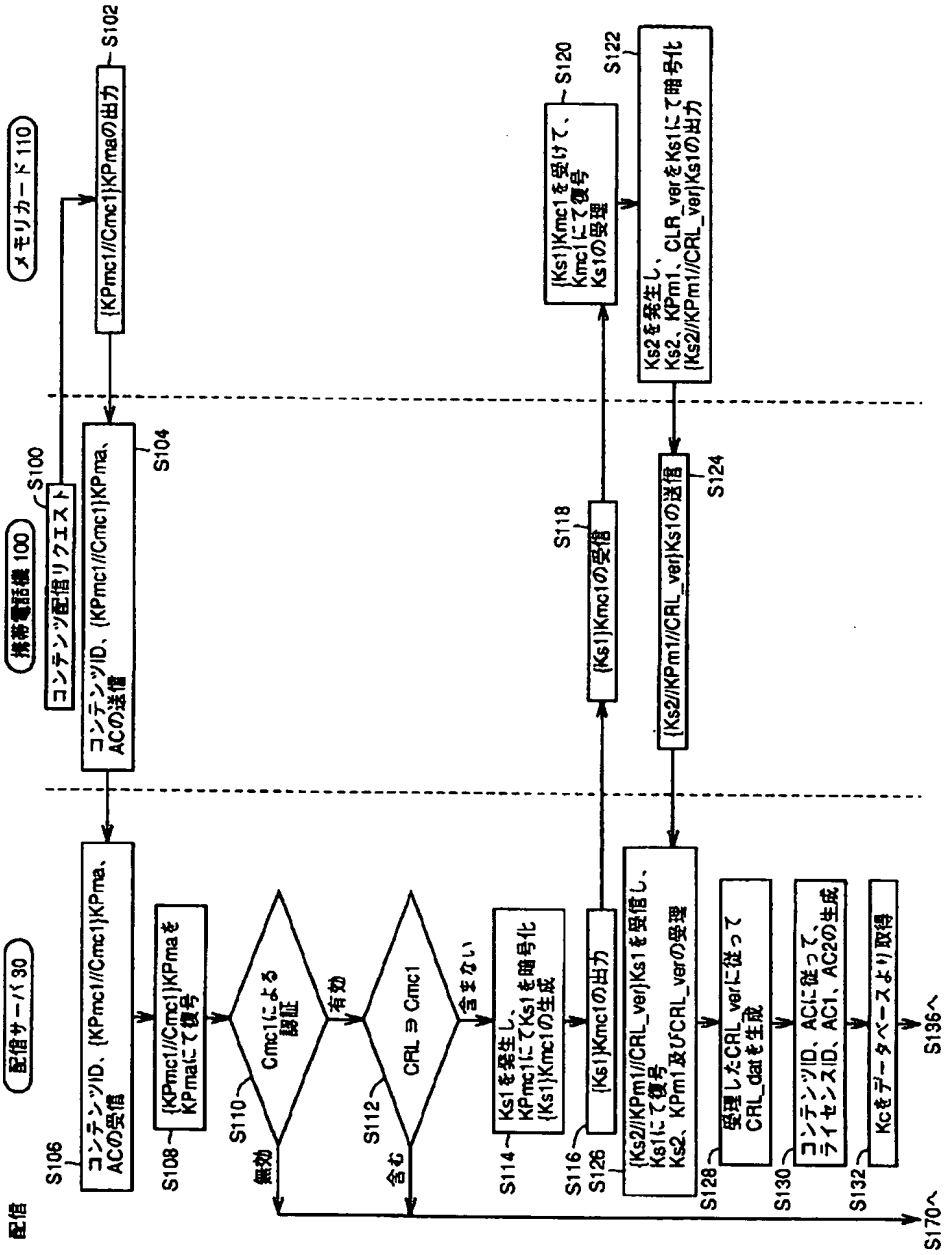
【図９】


110
1404
1406
1444
1408
1410
BS3
1201
1415
CRL
メモリ
{ライセンス}Km1
{Data}Kc
Data-Inf
復号 Kmc1
暗号化 Ks
復号 KPma
暗号化
復号 Ks
1412
コントローラ
1420
1402
Kmc1
KPma
1414
1442
Pd
Pb
Pc
Pa
1400
{KPmc1//Cmc1}KPma
1446
Pe
Pf
BS4
1422
復号 Km1
ライセンス情報 保持部
N
KPm1
Ks 発生
1416
1418
Km1
1421
1440
TRM

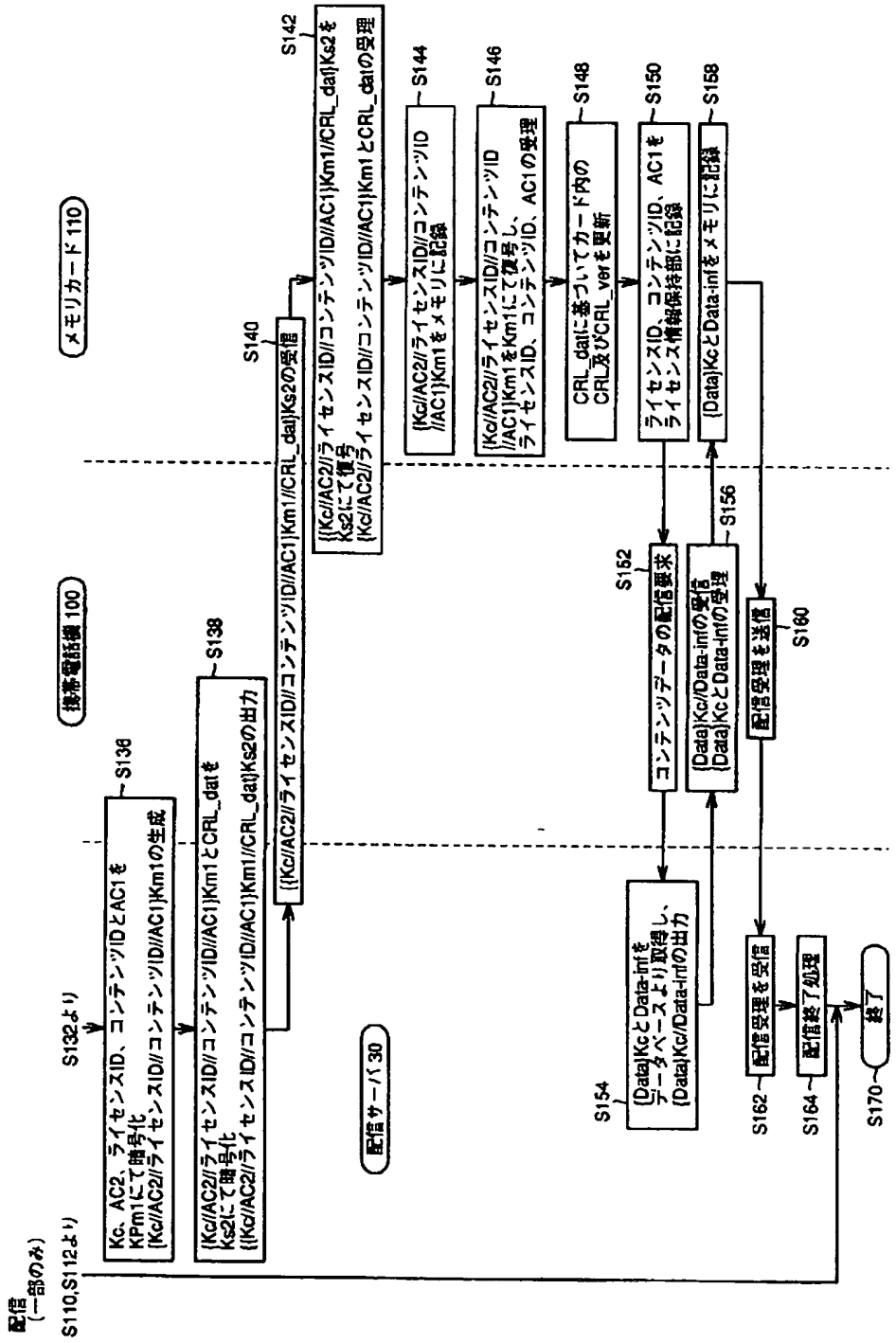
【図１２】


本体側処理
開始
利用者による再生指示
S200
S201
認証データ{KPp1//Crtf1}KPmaを メモリカードに入力
認証データ{KPp1//Crtf1}KPmaの受理 (KPp1とCrtf1の獲得)
S202
公開認証鍵KPmaにて復号
S203
S204
否
復号結果
可
S205
真
CRL ∋ Crtf1のID
S206
偽
認証データ不受理の出力
S207
再生不能の表示
メモリカード内処理

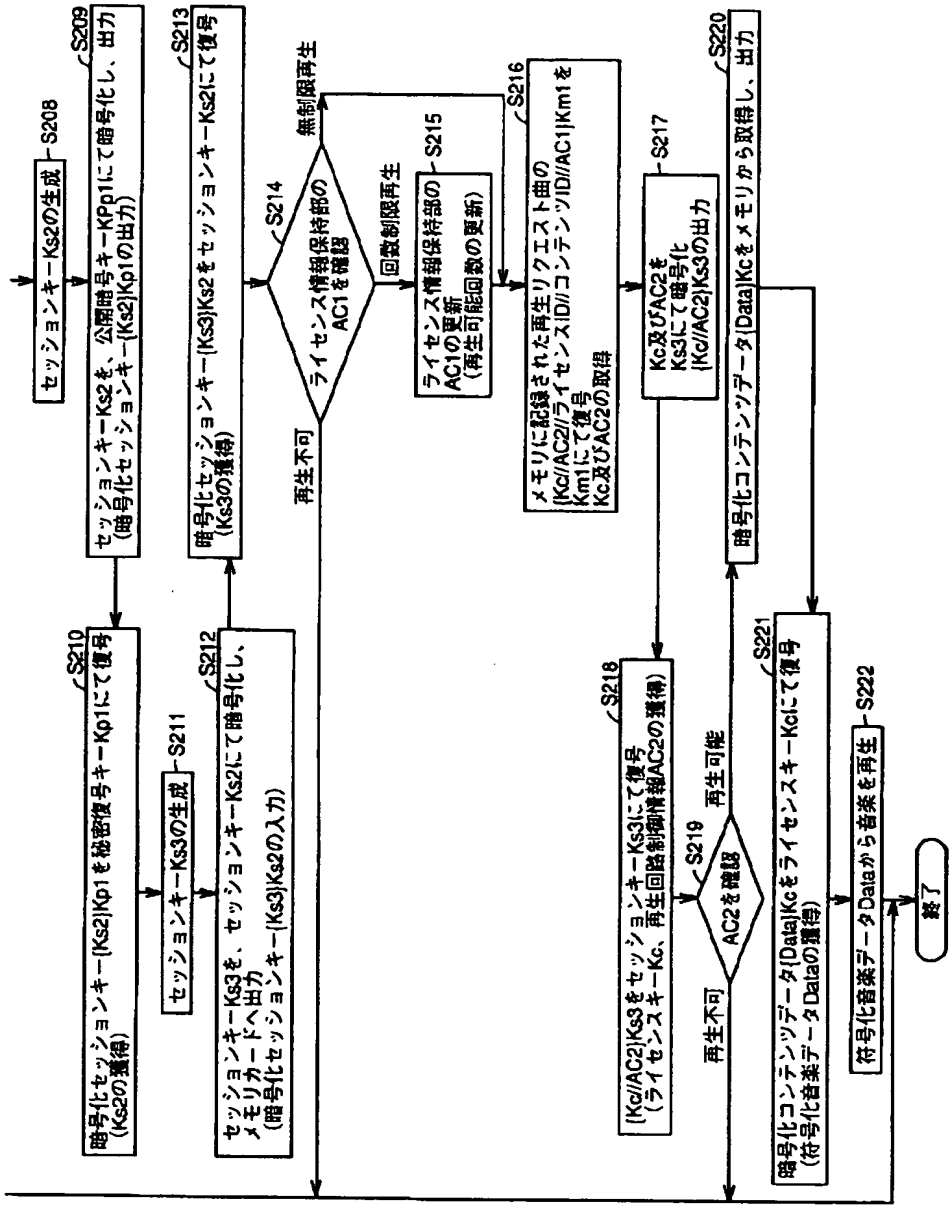
【図１０】


メモリカード 110
携帯電話機 100
配信サーバ 30
配信
S100
コンテンツ配信リクエスト
S102
{KPmc1//Cmc1}KPmaの出力
S104
コンテンツID、{KPmc1//Cmc1}KPma、ACの送信
S106
コンテンツID、{KPmc1//Cmc1}KPma、ACの受信
S108
{KPmc1//Cmc1}KPmaをKPmaにて復号
S110
Cmc1による認証
無効
有効
S112
CRL ∋ Cmc1
含む
含まない
S114
Ks1を発生し、KPmc1にてKs1を暗号化{Ks1}Kmc1の生成
S116
{Ks1}Kmc1の出力
S118
{Ks1}Kmc1の受信
S120
{Ks1}Kmc1を受け取て、Kmc1にて復号Ks1の受理
S122
Ks2を発生し、Ks2、KPm1、CLR_verをKs1にて暗号化{Ks2//KPm1//CRL_ver}Ks1の出力
S124
{Ks2//KPm1//CRL_ver}Ks1の送信
S126
{Ks2//KPm1//CRL_ver}Ks1を受信し、Ks1にて復号Ks2、KPm1及びCRL_verの受理
S128
受理したCRL_verに従ってCRL_datを生成
S130
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S132
Kcをデータベースより取得
S136へ
S170へ

【図１１】


メモリカード110
携帯電話機100
配信サーバ130
配信
(一部のみ)
S110,S112より
S132より
S136
Kc、AC2、ライセンスID、コンテンツIDとAC1を
KPm1にて暗号化
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1の生成
S138
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datを
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の出力
S140
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受信
S142
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datの受理
S144
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をメモリに記録
S146
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をKm1にて復号し、
ライセンスID、コンテンツID、AC1の受理
S148
CRL_datに基づいてカード内の
CRL及びCRL_verを更新
S150
ライセンスID、コンテンツID、AC1を
ライセンス情報保持部に記録
S158
{Data}KcとData-infをメモリに記録
S152
コンテンツデータの配信要求
S154
{Data}KcとData-infを
データベースより取得し、
{Data}Kc//Data-infの出力
S156
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S160
配信受理を送信
S162
配信受理を受信
S164
配信終了処理
S170
終了

【図１３】


セッションキーKs2の生成
S208
S209
セッションキーKs2を、公開暗号キーKP1にて暗号化し、出力
(暗号化セッションキー{Ks2}Kp1の出力)
S210
暗号化セッションキー{Ks2}Kp1を秘密復号キーKp1にて復号
(Ks2の獲得)
S211
セッションキーKs3の生成
S212
セッションキーKs3を、セッションキーKs2にて暗号化し、
メモリカードへ出力
(暗号化セッションキー{Ks3}Ks2の入力)
S213
暗号化セッションキー{Ks3}Ks2をセッションキーKs2にて復号
(Ks3の獲得)
S214
ライセンス情報保持部のAC1を確認
無制限再生
回数制限再生
再生不可
S215
ライセンス情報保持部のAC1の更新
(再生可能回数の更新)
S216
メモリに記録された再生リクエスト曲の
{Kc//AC2//ライセンスID//コンテンツID//AC1|Km1を
Km1にて復号
Kc及びAC2の取得
S217
Kc及びAC2を
Ks3にて暗号化
{Kc//AC2}Ks3の出力
S218
{Kc//AC2}Ks3をセッションキーKs3にて復号
(ライセンスキーKc、再生回路制御情報AC2の獲得)
S219
AC2を確認
再生可能
再生不可
S220
暗号化コンテンツデータ{Data}Kcをメモリから取得し、出力
S221
暗号化コンテンツデータ{Data}Kcをライセンスキー Kcにて復号
(符号化音楽データDataの獲得)
S222
符号化音楽データDataから音楽を再生
終了

【図１４】